Risk Measurement and Tools:

Some Qualitative and Semi-Quantitative Risk Metrics

The Critical Infrastructure Assurance Conference Series

Dallas Summit

JC Penney

15 May 2000

Revised: 11 May 2000

Daniel Harris

Information Security Specialist

Aon Corporation

Owings Mills, MD

The Measurement Problem -- I

- Risk analysis is an assessment of the exposures and management of the risk.
- “You cannot manage what you cannot measure.”
- Some risks cannot easily be measured, yet we must attempt to manage the risks.
- Information is the fundamental unit of business, yet it can be difficult to define and characterize.

The Measurement Problem -- II

- Traditional risk analysis is very difficult for information because of the following:
  - The value of information changes, depending on time, context, usage, and accessibility.
  - Many times information owners and custodians are unaware of the true value of the information.
  - Information may be aggregated from various sources.
  - The “threat-space” is constantly expanding.
  - Global connectivity, “anonymous” access, and distributed remote computing creates new challenges.

One Solution to the Measurement Problem

- Because it is so difficult to **accurately quantify** information risks, we must do the following:
  - audit our systems and procedures to find vulnerabilities.
  - mitigate risks by implementing current best practices (or promising practices).
- Qualitative and semi-quantitative indicators can provide an idea of risks and costs.
- Risk assessments deal with known risks, but there are always new risks and threats.
  - Use best practices to help protect against the unknown.
  - Best practices are real-world actions, policies, and controls to protect information systems.

AON

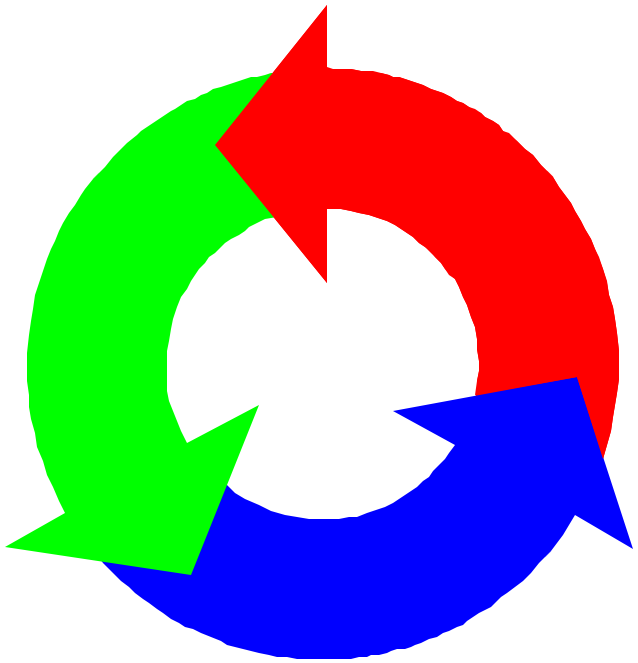
Why Measure Risks?

- Failure to **constantly** measure risks and understand the consequences could be disastrous.
- Many of the suggestions presented here are not traditional, numerical metrics, but rather these metrics are entities that can be measured or described.
  - They can provide insight into the risk posture of an organization.
  - These metrics provide data points in mapping a vulnerability profile and provide a place to start fixing serious vulnerabilities.

How Much is Enough?

- Because the game is always changing (new technologies and vulnerabilities), measuring, assessing, and mitigating the risks must be an on-going task.

Identify significant assets, interdependencies, and vulnerabilities.



Re-assess.

Remediate vulnerabilities.

Assess the Likely Targets of an Attack

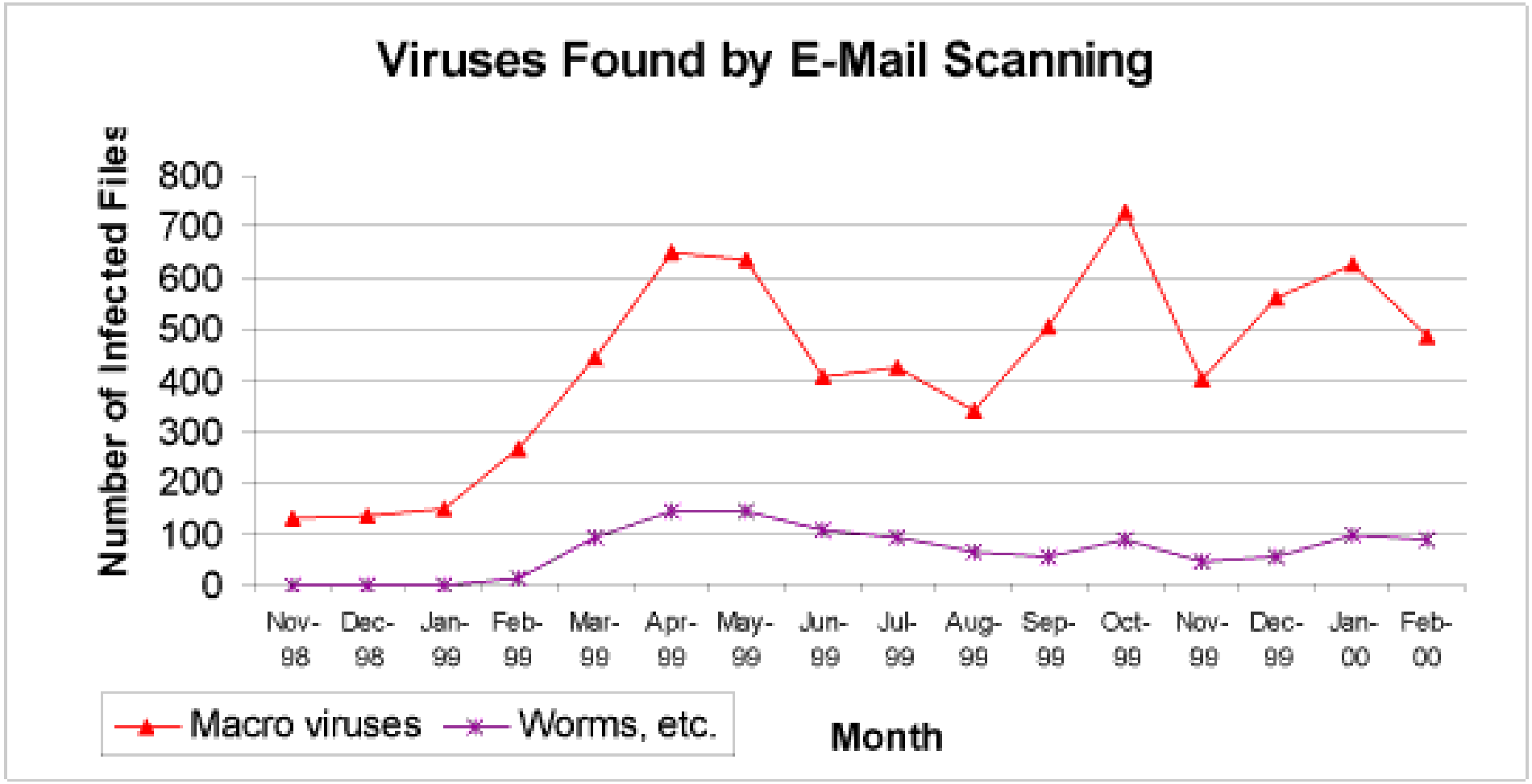
- Firewalls
- Routers
- Switches, hubs
- Servers
  - Web
  - File and Print
  - Application
  - Database
- Desktops
- Laptops
- PDA's
- Fax
- Modems and telephony infrastructure
- Employees
- Trash
- E-Mail
- Applications
- Connections to other networks
- The building & facilities
- The information "crown jewels"

AON

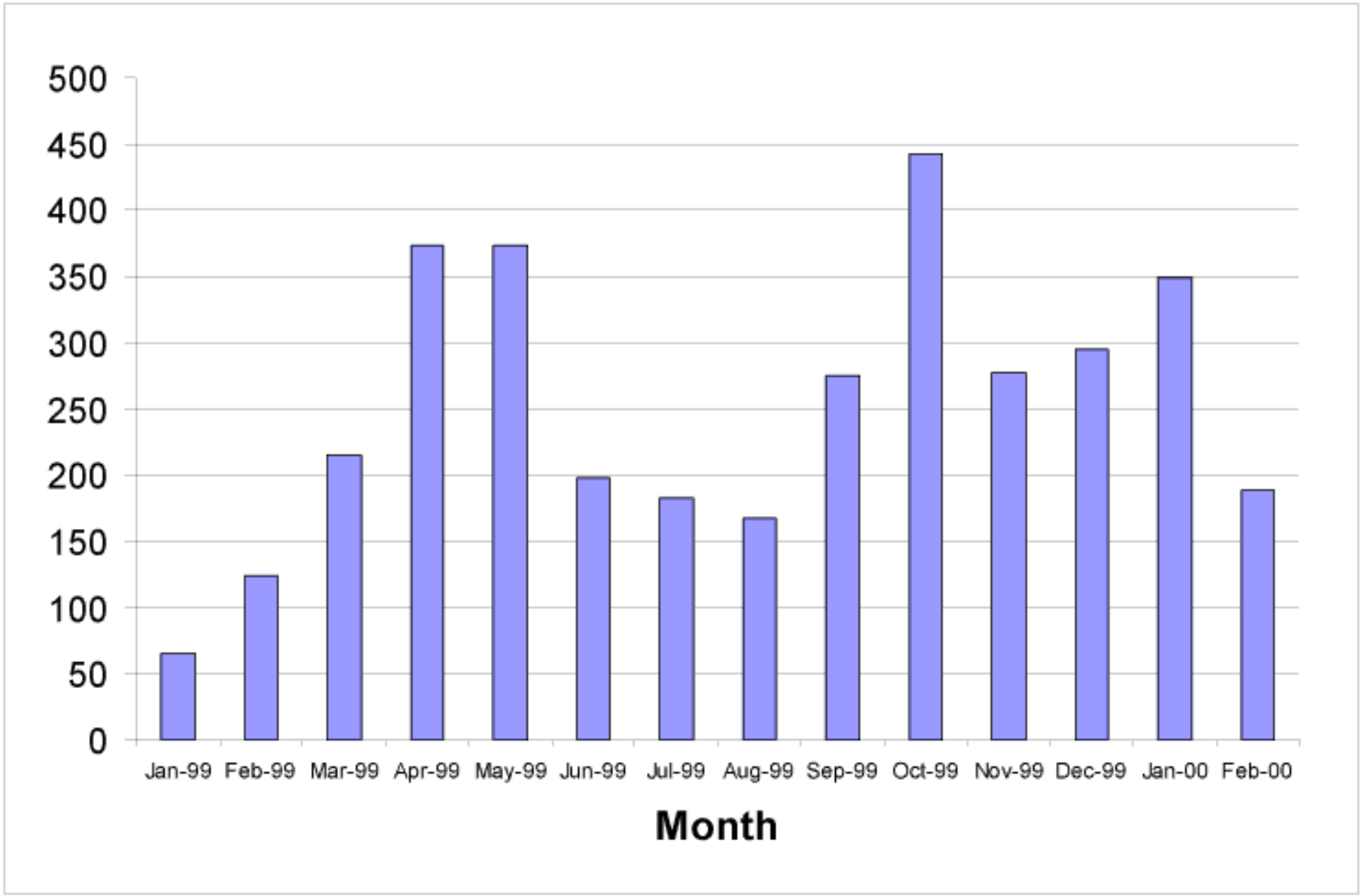
E-Mail Metrics

- E-Mail policy: up-to-date, understood, enforced?
- How many messages are sent daily?
  - inbound
  - outbound
- What are the permitted attachment types?
- Are there limits on the size of file attachments?
- How much E-Mail traffic is from attachments?
- Is message content scanned for information leakage and inappropriate content?
- How much traffic is non-business mail?

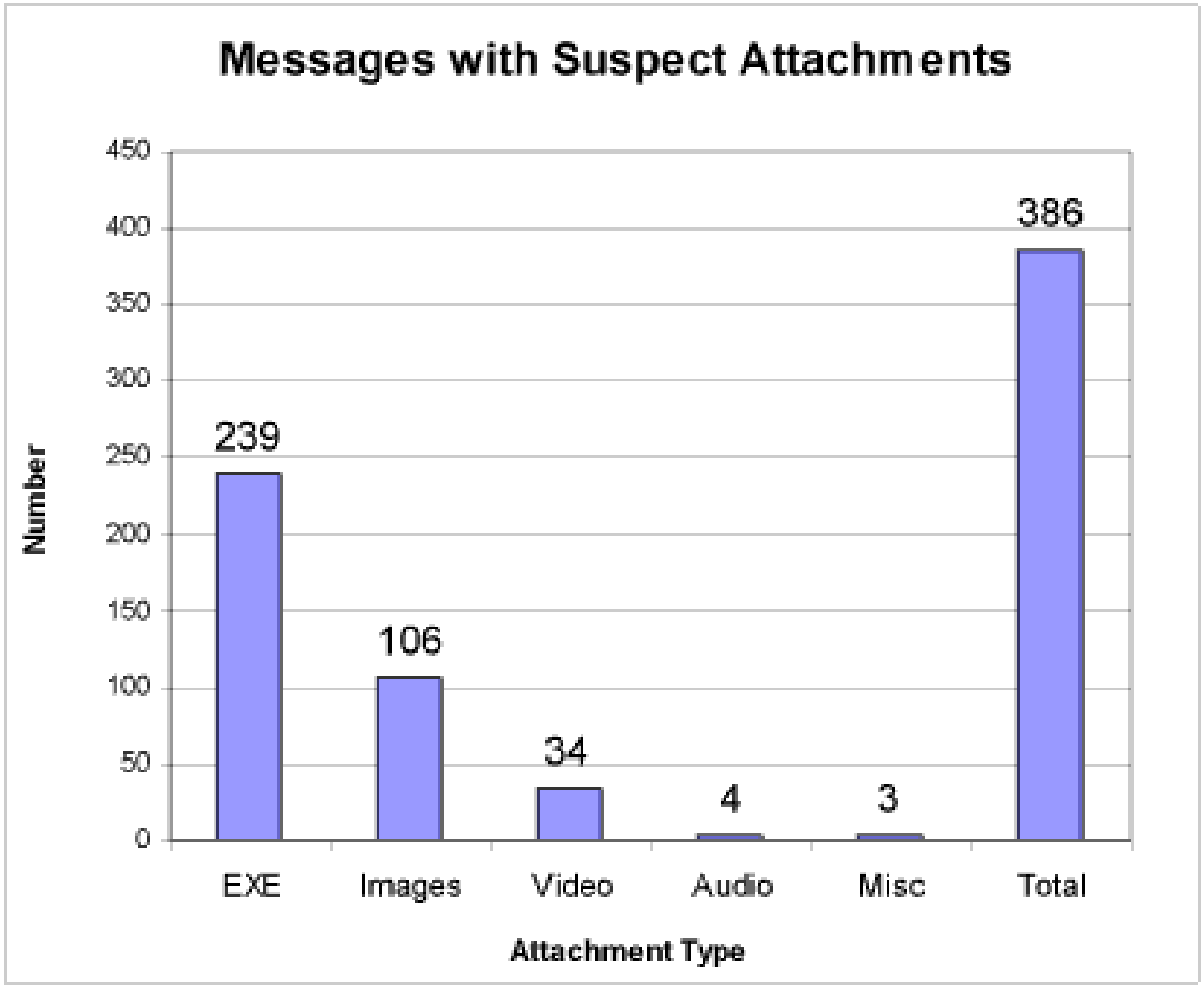
E-Mail Virus Scanning: The Real-World



Mail-Borne Viruses Stopped From Entering at the E-Mail Gateway



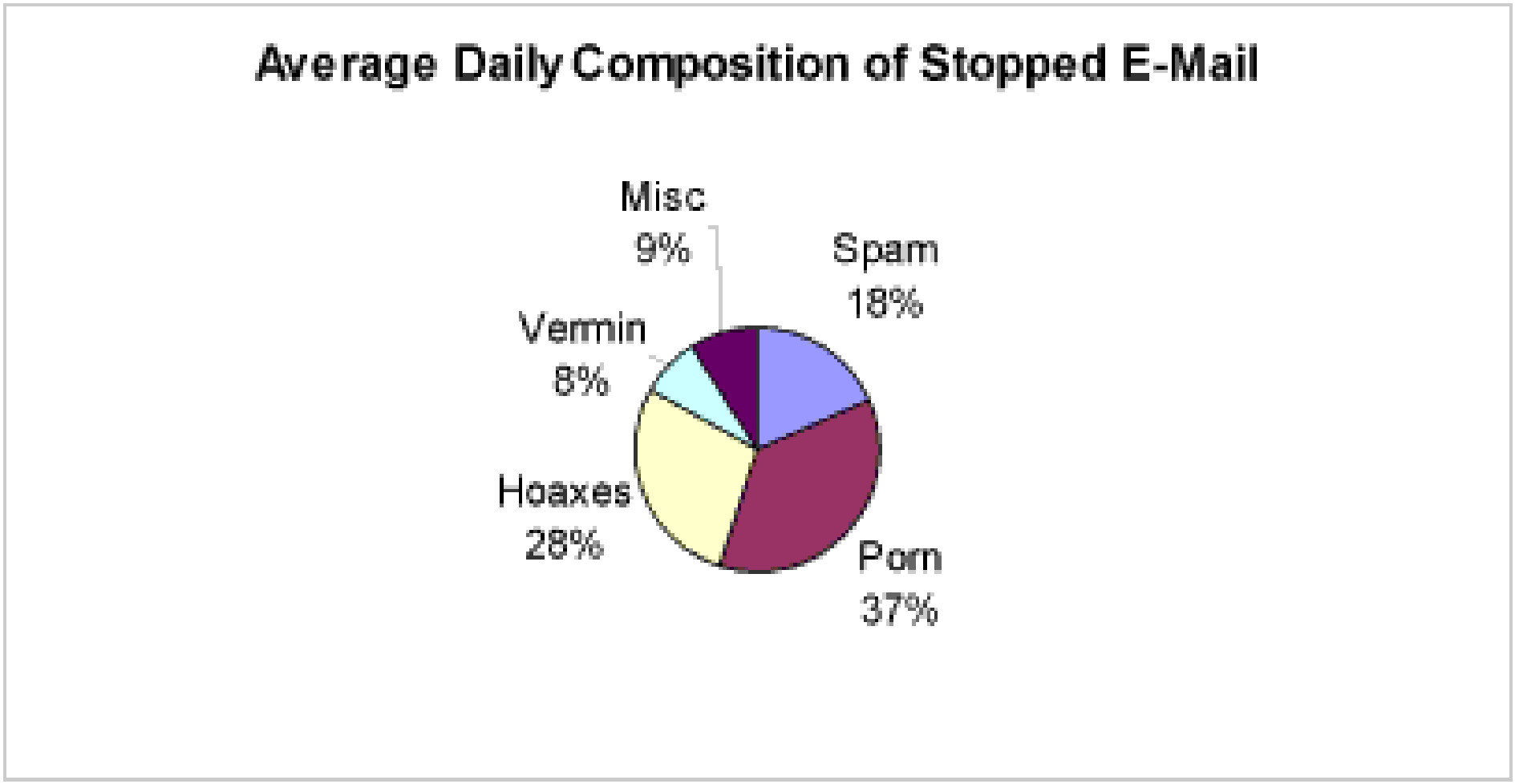
An Example of One Day's Worth of Suspect Attachments



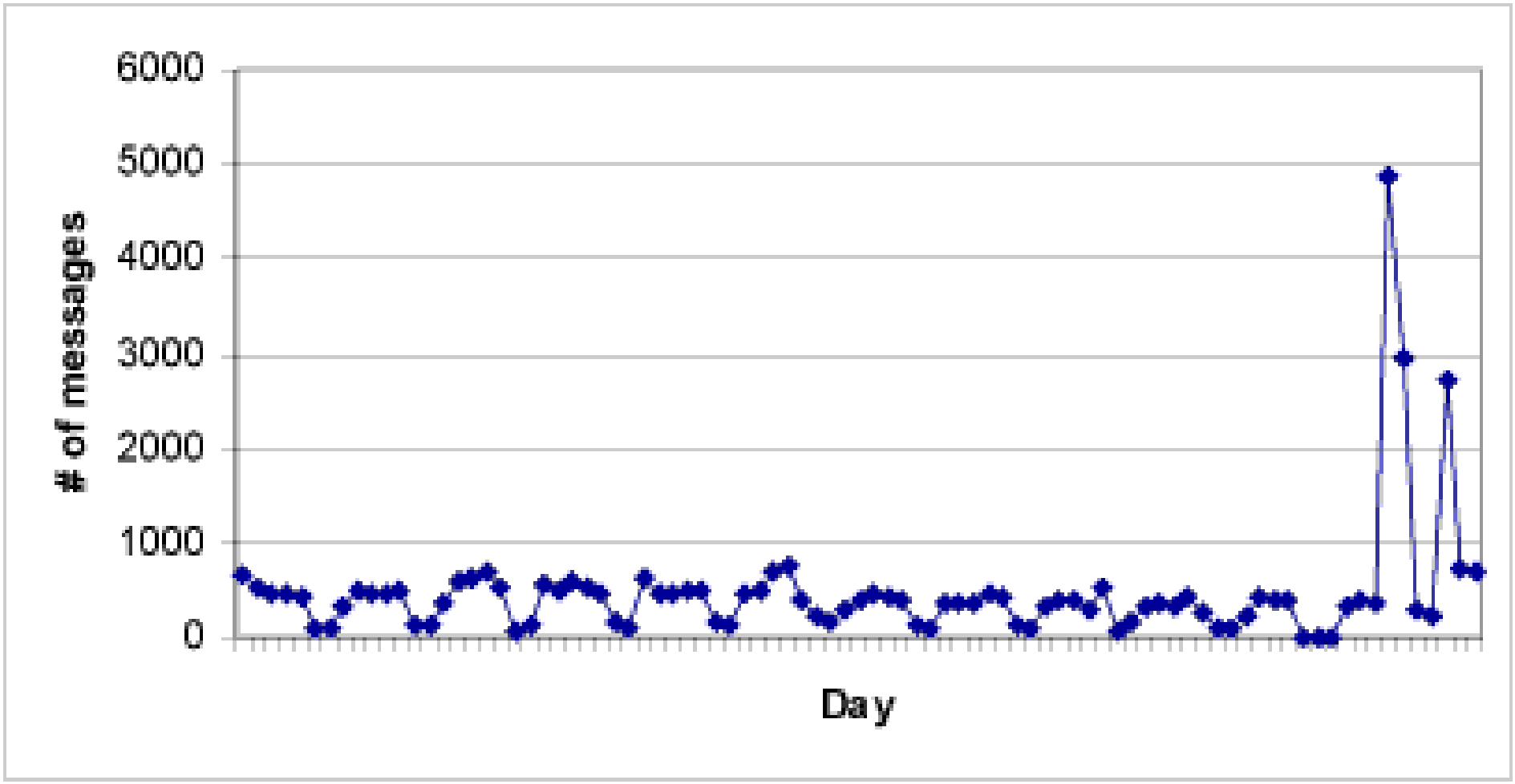
- 269 total suspect messages.
- 386 attachments.
- 335.3 Meg worth of suspect attachments.
- 107 messages originated from the inside.
- 345 Recipients.
- 245.6 Meg of traffic from internally generated messages.
- 162 messages originated from the outside.
- 89.7 Meg of traffic came in from the outside.

AON

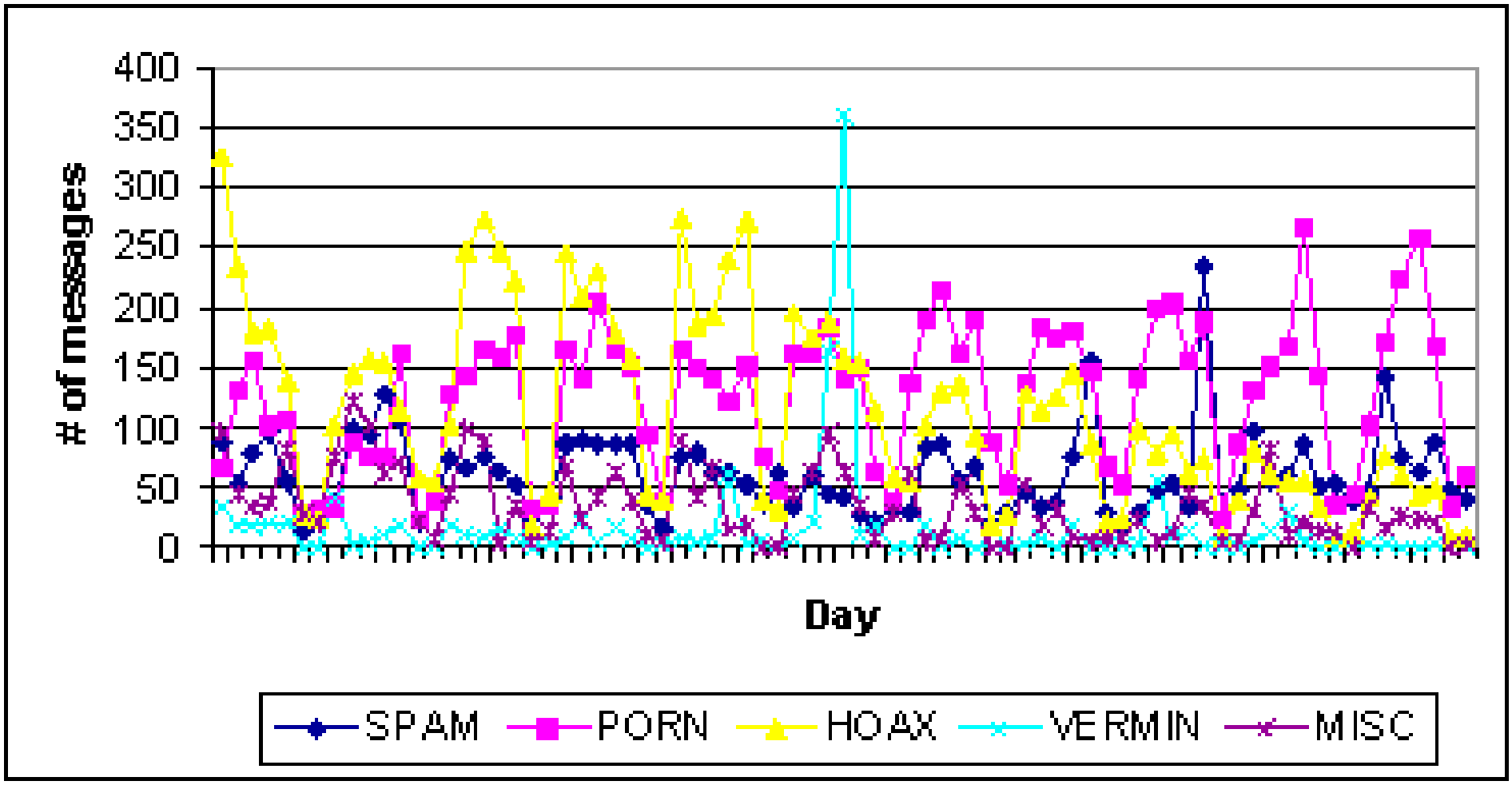
Non-Business Content



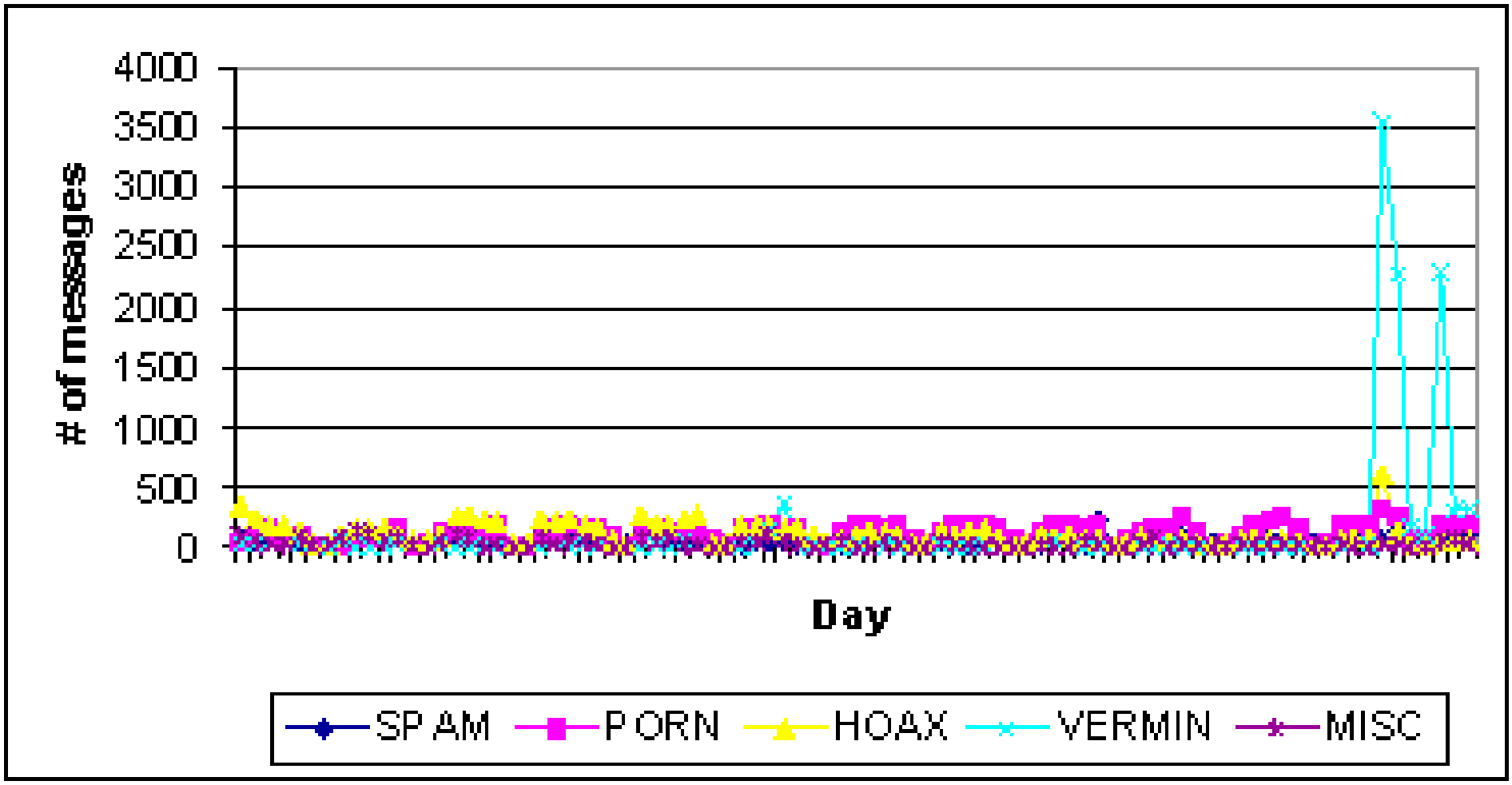
Stopped E-mail Messages (all types)



Stopped E-Mail Messages (before “Love”)



Stopped E-Mail Messages (after “Love”)



Virus Metrics

- Anti-Virus and software policies: up-to-date, understood, enforced?
- How many viruses are found at users' desktops?
- How many viruses are found at the E-Mail gateway?
- What are the top 10 viruses found at your organization?
- What is the source of most of the viruses (internal or external)?
- What is the average cost to clean and repair a single workstation in your organization?

Firewall Metrics

- Is the firewall architected with a DMZ?
- Which ports are open?
- What kinds of traffic are allowed?
- “There’s gold in them, thar logs!”
- Who are the top Internet users?
- What are the top applications?
- What is Internet traffic distribution by protocol (http, ftp, SMTP)?
- What are the top 500 websites?
- What kind of traffic is stopped?
- How much of each kind of traffic is stopped?

AON

Intrusion Detection

- How many Intrusion Detection incidents have been logged?
  - What kinds of incidents?
  - How many of each kind?
  - What severity level?
- What patterns or frequency?
- Are critical networks and systems being monitored for abuse and misuse?

E-Commerce Metrics

- How many websites are being run for your organization?
  - internal
  - external
- What kinds of content is stored on these websites?
  - public
  - proprietary
- Is the website transactional or informational?
- How many users have access to each website?
- How are users authenticated?
- How much traffic is generated by each website?

Operating Systems

- How homogeneous is your OS mix?
- What percentage of the systems are:
  - Windows?
  - Unix?
  - Mac?
- How often are systems scanned for known vulnerabilities?
- How are known vulnerabilities handled?
- How are vendor patches handled?
  - Update frequency, testing?
- Are the router operating systems up-to-date and patched?

Policy Metrics

- Is there a security policy that is promulgated and understood?
- How often are security awareness and training programs conducted?
- How is security information communicated to the field?
- What has corporate audit found?
- How many security incidents per month are logged?
- How many security investigations per year are logged?

AON

Miscellaneous Metrics

- How many calls to the help desk?
  - Number of password resets?
- What types of user authentication is used (re-usable passwords, tokens, biometrics)?
- How is remote access to networks done?
- How many third-party connections to/from your networks?
- How is data disposal handled?
- How many modems are on the network?

AON

Personnel Issues

- Are background checks conducted for sensitive IT positions?
- Are former hackers used to conduct vulnerability and penetration tests?
- How is access granted to information and network resources (permissive/restrictive)?
- How are non-employees (contractors, vendors) handled?
- Are Non-disclosure agreements (NDA's) signed by all users?

Information Security Best Practice Scorecard

	How are we doing?			
Information Security Current Best Practice	Not Using	Evaluating	In Pilot	Implemented
Firewalls				
Demilitarized Zone (DMZ)				
Intrusion detection				
Ingress & Egress filtering				
E-Mail content filtering				
E-Mail attachment filtering				
Secure E-Mail				
Proxy server with user authentication				
Web URL blocking				
Active content filtering				
RFC 1918 addressing				
Incident response handling				
User awareness & training				
Security policies & procedures				
Ongoing vulnerability assessment and audit program				

AON

Commonly Exploited Vulnerabilities Scorecard

	How are we doing?				
Common Vulnerabilities	**Unaware of the issue**	**Aware of the issue**	**N/A**	**Patching systems**	**All systems patched**
Denial of Service					
Weak accounts					
IIS weaknesses					
Open databases					
E-business web applications					
Open E-Mail					
File sharing					
RPC vulnerabilities					
BIND					
Linux buffer overflows					

- Source: **ISSalert: Top 10 Vulnerabilities**, E-Mail from xforce@issnet, 09 May 2000
- Compare the findings in your organization to other organizations.
  - http://www.cisco.com/warp/public/778/security/vuln_stats_02-03-00.html

AON

Newly-Found Vulnerability Scorecard

	How are we doing?				
New Vulnerabilities	Unaware of the issue	Aware of the issue	N/A	Patching systems	All systems patched

- This information should be used to create a vulnerability profile to determine what areas need remediation.
- New vulnerabilities are constantly being developed; therefore, there is a need to continuously measure and assess vulnerabilities.
- See http://www.nipc.gov/cybernotes.htm for a nice list of newly-found vulnerabilities (published every 2 weeks).

AON

Benchmark Your Organization

- Develop a baseline profile.
- If the kinds of metrics described here and vulnerability assessments indicate that action is required, then:
  - Prioritize the issues.
  - Set goals for improvement.
  - Fix the vulnerabilities and apply best practices. For example, see http://www.sans.org/newlook/resources/esa.htm
- Add new metrics as they become apparent.
- Track the metrics over time to monitor the effectiveness of the audit and vulnerability assessments.
- Stay aware of new vulnerabilities and best practices.
- Compare how your organization is doing versus other organizations with published metrics.
  www.cisco.com/warp/public/778/security/vuln_stats_02-03-00.htm

AON

What You Can Do

- Show the organization that security is taken seriously.
- Many of the metrics mentioned here are relatively easy to obtain.
  - Ask to see the numbers!
- Use assessment tools and automated processes to measure parameters where ever possible.
- Involve audit and the security groups.
- Use the metrics to find areas that can be addressed first with high impact, low cost solutions.
- Security is an on-going process of education and continuous improvement.

AON